Cyber Security: On the Front Line:

Securing the Home Computer and Reporting Internet Crime

February 2011

Securing the Home Computer

Setting up a new computer usually entails more than taking it out of a box and plugging it in. This is especially true if the new computer is a replacement for an existing computer and/or there will be a transfer of data or programs from one computer to another.

The successful transition to a new computer requires some pre-planning and can include protecting legacy data, transferring important files, setting up a new optimal computer environment, and disposing of old equipment.

At DOE, EITS is responsible for migrating EITS customers to new work computers. EITS plans, schedules, and carries out equipment transitions in a way that minimizes impacts to the customer.

EITS users are generally unaware of the many activities and the amount of coordination required for a smooth transition from one computer to another such that data is protected and negative impacts to user productivity minimized.

Just as EITS manages the migration to new technologies at work, the user must similarly manage and plan the transition to a new computer at home.

Important steps to take when moving to a new computer include:

- **Creating a Data Backup** to preserve legacy data and software
- **Preparing the New Computer** by establishing a safe and secure environment; and
- **Properly Disposing of the Old Computer** by removing legacy data and properly recycling the equipment.

Create a Data Backup:

The first step in transitioning to a new computer is to create a current backup of the desired data on the legacy computer.

The user should always maintain a backup of important files separate from the computer itself. A complete backup creates a copy of the entire hard drive, which can be used to restore a computer to a "safe" state should a problem occur. The user should maintain a current complete backup in a safe place.

There are many data backup options. These include "backing up" or "copying" relevant files to an external hard drive, separate networked drive, a commercial network backup service, a large capacity thumb drive, or CDs /DVDs. The type of storage media used is a function of the amount of storage needed, the level of security desired, the degree of mobile access required, and the availability, convenience, and cost of the different options.

The backup and copy utilities that are part of the standard computer system can be used to backup files. Alternately, storage devices such as external hard drives may come with a suite of storage management utilities such as backup, restore, encryption and password protection.

Once a complete backup is available, the user should review the legacy computer and identify data files and programs desired for the new computer. Data files are the primary files that are transferred between computers. This includes document, audio, image, and video files. The selected data files should be copied to storage media for transfer. The source files and documentation for legacy programs to be installed on the new computer should be assembled. Some programs may not be compatible with the new computer environment.

Work files should be maintained separate from personal files on a home computer, and they should be deleted when no longer needed. When transferring files to a new home computer, work files should be reviewed to determine whether they are still relevant or need to be preserved for work purposes. Do not copy unnecessary work files to a home computer.

It is Best Practice to maintain Federal work files on Federal equipment. Ideally, DOE work files should be stored on DOE computers, network drives, or DOE-provided storage device such as a thumb drive or CD.

Help Desk numbers

Headquarters & Richland:
- Phone: 301-903-2500
- Toll Free: 866-834-6246
- Email: ESC.ServiceDesk@hq.doe.gov
- Web (DOE internal): http://eits.doe.gov/service_desk/frmHelpDesk1.cfm

Other Field Locations:
- Phone: 505-845-4357
- Toll Free: 888-231-5529
- Email: EnterpriseServiceCenter@doeal.gov

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

Prepare the New Computer:

Be Organized

Shared or family computers:

- **Set the computer up in an open space** to help monitor online activities.
- **Create a separate computer account for each user** and manage account administrative rights and protections for young family members**.**
- **Remember to Password Protect adult accounts.** Keep passwords in a secure place, away from the computer space and children.
- **Maintain a clean workspace.** Do not leave sensitive information, such as SS#, credit card numbers, and financial information where others can find it or have access. Remove sensitive materials from the computer workspace.
- **Use external storage** for important and sensitive information and keep external storage devices in a secure location.
- **Keep an active backup.**

Computers used for both home and work:

- **Maintain separate accounts for work and home activities performed on a single computer.** Store work information separate from personal information.
- **Use external storage for work data** to maintain the security and integrity of work data. Work data can be stored on the DOE network servers, external hard drives, thumb drives, or CD/DVDs.

Maintain Important Records:

It is important to secure copies of vital system information and programs in case of system failure.

Establish a Document and Software Library

- **Collect and store all documentation and relevant information on a system**. Keep receipts, serial numbers, administration information, warranties, and passwords. Include Help Desk and customer service numbers and incident information.
- **Collect and store all hardware and software manuals, CDs, and DVDs.** Create a CD or DVD copy of all OS, software, and other vital files (such as drivers) for which none exist, including those files downloaded from the internet.

Keep all relevant program documentation and copies of internet documentation or emails.

Start Secure/Stay Secure

- **Install, maintain, and run comprehensive security software that includes**:
  - anti-viral, anti-spyware, and malware
  - firewall protection
  - email and spam blocking
  - automatic alerts and updates
- **Do not download free software unless it is from a trusted source and trusted site.** Be cautious of downloads unless you can verify the integrity of the source and the authenticity and security of the site. Be wary of "free" security software as these are common "bait".
- **Use strong passwords and change them on a regular basis.** Use different passwords for different accounts; do not use the same username and password on numerous sites. Use different passwords for work and personal purposes.
- **Set software to check for updates on an automatic and regular basis**. Any installed software can be a threat to a computer system, and a security issue with one program can impact another. Patches or updates for security issues are critical to system security; therefore, installing software patches and updates as they become available is always a priority.

Safety On and off the Grid:

- **Always use a surge protector** to prevent power surges from corrupting computer files.
- **Use an UPS** (uninterrupted power supply), if power interruption is a common risk.
- **Turn off the computer and surge protector when not in use**, in order to conserve energy.
- **Always disconnect the internet when not in use,** to prevent unauthorized internet traffic.
- **Ensure sufficient airflow** around the computer to prevent over-heating. Use auxiliary air circulation for laptops, if needed.

For comments, corrections, or suggestions for future Front Lines, send an email to CRB@hq.doe.gov.

Properly Dispose of the Old Computer:

Clean

Clean computers of all data before disposal to protect personal, financial, and other sensitive information from disclosure to others and to prevent unauthorized use. Even if a computer is not operable and the user is unable to access data, large volumes of data may be recoverable from the computer hard drives using basic skills and simple tools.

Users should not rely on the standard computer "reformat" utility to clean a hard drive of data preliminary to disposal as this process does not remove the data. More effective and secure options are:

- **Remove the hard drive and store it in a secure place** (perhaps as a backup or for later use).
- **Remove the hard drive and physically destroy it**. This includes drilling holes or smashing.
- **Use hard-drive wipe software** to encrypt or permanently delete the data.
- **Use a reformat or wipe utility on the hard drive, and then remove and physically destroy it.**

Recycle

Recycle your electronics: It is easier than you might think!

After the computer is "cleaned" of data, recycle choices depend on the residual operability or value of the equipment. Clean and operable computers can be donated or given to others.

Web networks, such as **www.freecycle.org**, promote recycle by facilitating reuse and sharing of useable items, including computers.

If the computer has no operable value, it can be disposed of through an e-cycling program. Computers contain toxic and hazardous materials that are potentially harmful to the environment and the public. Therefore, federal law mandates the proper disposal of computers and other electronic equipment.

The EPA established a network of companies to facilitate the recycle and safe disposition of consumer electronics. In addition to computers, the partners accept DVD players, TVs, cell phones, microwaves, and other consumer electronic goods.

The "Recycle Partners" vary in the types of electronics accepted and the collection process used (e.g. drop off centers or mail-in).

A complete list of Recycle Partners and detailed information on the individual programs is available on the EPA "Plug-In to eCycling" Partners website:

http://www.epa.gov/epawaste/partnerships/plugin/partners.htm.

Help Desk numbers

Headquarters & Richland:

- Phone: 301-903-2500
- Toll Free: 866-834-6246
- Email: ESC.ServiceDesk@hq.doe.gov
- Web (DOE internal):

http://eits.doe.gov/service_desk/frmHelpDesk1.cfm

Other Field Locations:

- Phone: 505-845-4357
- Toll Free: 888-231-5529
- Email: EnterpriseServiceCenter@doeal.gov

Reporting Internet Crime

In November 2010, EITS sponsored Cyber Security Awareness Days at Germantown and Forrestal. At these events, Internet Crime was a popular topic of interest.

The Internet Crime Complaint Center (IC3) is the multi-agency alliance and clearinghouse for reporting and investigating internet crime.

If you believe you have been a victim of internet crime or are suspicious of specific internet traffic, report the activity to the IC3 at the web site www.ic3.com.

The IC3 web site also provides basic information on common internet crimes, how to identify internet crime, and steps to avoid becoming a victim.

The Federal Trade Commission (FTC) website also has valuable information on internet crime. For FTC consumer information specific to internet fraud and abuse visit: **www.ftc.gov/bcp/menus/consumer/tech.shtm**

For comments, corrections, or suggestions for future Front Lines, send an email to CRB@hq.doe.gov.

Internet Crime Complaint Center

Data, Tools, and Resources for Enforcement Professionals

The Internet Crime Complaint Center (IC3) is an alliance between the National White Collar Crime Center (NW3C) and the Federal Bureau of Investigation (FBI). IC3's mission is to address crime committed over the Internet. For victims of Internet crime, IC3 provides a convenient and easy way to alert authorities of a suspected violation. For law enforcement and regulatory agencies, IC3 offers a central repository for complaints related to Internet crime, uses the information to quantify patterns, and provides timely statistical data of current trends.

Features

- Provides a central point for Internet crime victims to report and to alert an appropriate agency on-line at **www.ic3.gov**
- Collects, reviews, and refers Internet crime complaints to law enforcement agencies with jurisdiction to aid in preventive and investigative efforts
- Identifies current crime trends over the Internet

Benefits

- Provides an analytical repository for Internet crime complaints
- Analyzes and refers all fraudulent activity identified on the Internet to the appropriate local, state, or federal law enforcement authority
- Aids in the development of law enforcement training to address identified Internet crime problems
- Serves as the catalyst that allows law enforcement and regulatory agencies to network and share data
- Potentially reduces the amount of economic loss by Internet crime throughout the United States

To file an Internet crime complaint, visit the IC3 Web site at www.ic3.gov.

NW3C
NATIONAL WHITE COLLAR CRIME CENTER
INTEGRITY QUALITY SERVICE

August 2005